U.S. Application 09/724,459 **Examiner Paul E. Callahan**

Proposed new claims after the interview with the Examiner on August 12, 2002

74. A method of authenticating a dispatch and contents of the dispatch transmitted from a sender to a recipient, comprising the steps of:

sending content data representative of the contents of the dispatch, and a destination of the dispatch associated with said recipient, to an authenticator functioning as a non-interested third party with respect to the sender and the recipient, to be forwarded to said destination;

receiving a representation of authentication data that has been generated by said authenticator, said authentication data comprising a representation of the following set A of information elements: a_1 - comprising said content data, and dispatch record data elements $a_2,..., a_n$ which includes at least an indicia a_2 relating to a time of the dispatch which is provided in a manner resistant to or indicative of tampering by either of the sender and the recipient, and an indicia a_3 relating to said destination of the dispatch,

wherein at least part of said authentication data is secured against tampering of the sender and the recipient, and

wherein said authentication data includes a set B comprising one or more information elements $b_1,..., b_m$, each element b_i comprising a representation expressive as a function F_i of a subset S_i of a selected portion of said set A, and where said functions F_i and subsets S_i can be different, and

wherein said authentication data does not comprise an encrypted representation of said content data and said dispatch record data which is encrypted with a secret key, either symmetric or asymmetric, associated with said recipient.

75. Authentication data for authenticating a dispatch and contents of the dispatch electronically transmitted from or for a sender to a recipient, comprising a representation of a selected portion of the following set A of information elements:

content data a_1 representative of the contents of a dispatch; and

dispatch record data elements $a_2,..., a_n$ which include at least an indicia a_2 relating to a time of the dispatch and an indicia a_3 relating to the destination of the dispatch,

wherein said time related indicia a_2 being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient, and

wherein at least part of said authentication data is secured against tampering of the sender and the recipient, and

wherein said authentication data are generated and secured by an authenticator functioning as a non-interested third party with respect to the sender and the recipient, and

wherein said authentication data includes a set B comprising one or more information elements $b_1,..., b_m$, each element b_i comprising a representation expressive as a function F_i of a subset S_i of a selected portion of said set A, and where said functions F_i and subsets S_i can be different, and

wherein said authentication data does not comprise an encrypted representation of said content data and said dispatch record data which is encrypted with a secret key, either symmetric or asymmetric, associated with said recipient.

76. A method for verifying the authenticity of a dispatch sent from a sender to a recipient, comprising the steps of:

providing a representation of a selected portion of a group A' of elements purported authentic, and which includes a content data, and dispatch record data comprising at least a time and destination relating to the dispatch;

verifying said representation for match with a representation of at least part of authentication data, that has been generated by an authenticator functioning as a non-interested third party with respect to the sender and the recipient, said authentication data comprising a representation of the following set A of information elements: a_1 - comprising said content data, and dispatch record data elements $a_2,..., a_n$ which includes at least an indicia a_2 relating to a time of the dispatch which is provided in a manner resistant to or indicative of tampering by either of the sender and the recipient, and an indicia a_3 relating to said destination of the dispatch,

wherein at least part of said authentication data is secured against tampering of the sender and the recipient, and

wherein said authentication data includes a set B comprising one or more information elements $b_1,..., b_m$, each element b_i comprising a representation expressive as a function F_i of a subset S_i of a selected portion of said set A, and where said functions F_i and subsets S_i can be different, and

wherein said authentication data does not comprise an encrypted representation of said content data and said dispatch record data which is encrypted with a secret key, either symmetric or asymmetric, associated with said recipient.